Java4Shell: compensating-control checklist

CVE-2026-114938 | Cyber Insights | November 20, 2026

For authorized service owners. Temporary controls complement a supported runtime fix. This checklist does not certify WAF efficacy or establish that a workload is free of compromise.

1. Establish scope

Record service, runtime vendor/build, exposed paths, supported product guidance and owner. Include non-HTTP integrations and recovery instances.

2. Prove the boundary

Confirm traffic passes through the selected enforcement point. Review inspection limits, parsing, encrypted visibility, exceptions, rule order and effective action.

3. Test operational safety

Use staging and synthetic data. Check legitimate transactions, logging, enforcement plumbing and rollback. Observation/count mode is not blocking protection.

4. Record residual risk

Define what the control covers, what remains unknown, who accepts the exception, its expiry and the supported patching plan.

Control	Evidence to collect	Limit to retain
WAF / boundary filter	Policy revision, protected route, enforced action, functional tests	Not a generic proof against every input path
Network restriction	Approved reachable clients, origin rules, tested business access	Reachability reduction does not repair code
Runtime mitigation / fix	Supplier guidance, running-process setting or fixed build, restart	Check all nodes; no claim about prior compromise
Monitoring / endpoint controls	Collection coverage, timestamps, correlated leads and disposition	Absence of an alert is not proof of safety

Service / owner: _____

Evidence / reviewer: _____

Exception expiry / patch change: _____

Read the full guide and primary sources at cyberinsights.ca

Retire temporary measures through change control after verified permanent remediation. Keep incident assessment separate.